AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A message encryption system comprising:

a session key employed to securely exchange a message associated with a dialog; and,

an encryption component that employs asymmetric encryption to first securely transmit the session key, the session key thereafter being employed to encrypt the message and securely exchange the message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message, the message comprises a digital certificate that is employed as part of a broker service security system that facilitates location transparency of services by creating a remote service binding which addresses a service by a logical name such that an application can utilize the service independent of the physical location of the service.

2. (Original) The system of claim 1, the session key comprising a 128-bit randomly generated symmetric key.

3. (Original) The system of claim 1, the encryption component first encrypts the session key employing a private key, the encryption component further encrypts the result of the first encryption employing a public key.

4. (Cancelled).

5. (Original) The system of claim 3, the public key being associated with a target of the message.

6. (Original) The system of claim 3, further comprising a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key.

7. (Original) The system of claim 6, a trusted agent negotiates a unique session key with a subscriber

8. (Original) The system of claim 6, the trusted agents acting in concert to dynamically load balance distribution for the publisher.

9. (Original) The system of claim 3, the public key being stored as a digital certificate.

10. (Original) The system of claim 9, the digital certificate being associated with a user *via* a login protocol.

11. (Original) The system of claim 1, the encryption component first encrypts the session key employing a private key, the encryption component further encrypts the result of the first encryption employing a public key, and, the encryption component separately encrypts the session key with a public key, the result of the second encryption and the separate encryption provided as an output.

12-13. (Cancelled).

14. (Currently Amended) A message decryption system comprising:

a session key employed to securely exchange a message associated with a dialog; and,

a decryption component that employs asymmetric decryption to first securely decrypt the session key, the session key thereafter being employed to decrypt the message, wherein the session key encrypted message is first decrypted using a public key securely associated with an initiator of the message, the message comprises a digital certificate that is employed as part of a broker service security system that facilitates location transparency of services by creating a

remote service binding such that an application can utilize the service independent of the physical location of the service.

15. (Original) The system of claim 14, the decryption component first decrypts a message with a private key, the decryption component further decrypting the result of the first decryption with a public key, the result of the second decryption is the session key.

16. (Original) The system of claim 15, the private key being securely associated with a target of the message.

17. (Cancelled)

18. (Currently Amended) A method facilitating session key encryption comprising:

firstly encrypting a symmetric session key with a private key;

secondly encrypting a result of the first encryption with a public key; and,

providing a result of the second encryption as an output, the output comprises a digital certificate that is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service.

19. (Original) The method of claim 18, the private key being associated with an initiator of a message.

20. (Original) The method of claim 18, the public key being associated with a target of a message.

21. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 18.

22. (Currently Amended) A method facilitating session key decryption comprising:

firstly decrypting a message with a private key;

second decrypting a result of the first decryption with a public key; and,

employing a result of the second decryption as a session key, the session key thereafter being employed to decrypt ~~the~~ a subsequent message, wherein the ~~session key encrypted~~ subsequent message is first decrypted using a public key securely associated with an initiator of the message;

facilitating location transparency of services within a service broker security system employing a digital certificate included in the subsequent message by creating a remote service binding that addresses the broker service logically by name such that an application can utilize the broker service independent of the physical location of the service;

deploying multiple instances of the service broker;

sharing the private key within the multiple instances of the service broker; and

negotiating a unique session key with each of a subscriber accessing an instance of the service broker.

23. (Original) The method of claim 22, the private key being associated with a target of a message.

24. (Original) The method of claim 22, the public key being associated with an initiator of a message.

25. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 22.

26. (Currently Amended) A computer-readable medium encoded with a data structure that facilitates secure distributed communication, the data structure comprising:

a data field comprising an encrypted message, the encrypted message first encrypted with a symmetric session key, then encrypted with a private key securely associated with an initiator of the message, the message comprises a digital certificate that is employed as part of a service broker security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service.

27. (Currently Amended) A message decryption system comprising:

means for receiving an encrypted session key;

means for decrypting the encrypted session key using a private key;

means for decrypting a result of the first decryption with a public key;

means for securely storing a result of the second decryption as a session key;

means for employing the session key to decrypt a message, wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message; and,

means for employing a digital certificate included in the message to create ~~creating~~ a remote service binding such that an application can utilize the service independent of the physical location of the service.

28. (Previously Presented) The system of claim 1, further comprising multiple instances of the broker service sharing the same private key such that the application treats the multiple instances collectively as a unit.